

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

XIAOXING XI, *et al.*,

Plaintiffs,

v.

Civil Action No. 17-2132

FBI SPECIAL AGENT ANDREW  
HAUGEN, *et al.*,

Defendants.

**THE GOVERNMENT’S MOTION TO DISMISS PLAINTIFFS’ CLAIMS  
AGAINST OFFICIAL CAPACITY DEFENDANTS CHRISTOPHER A. WRAY,  
JEFFERSON B. SESSIONS, III, AND ADM. MICHAEL S. ROGERS**

Pursuant to Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure, defendants Christopher A. Wray, Jefferson B. Sessions III, and Adm. Michael S. Rogers (the “Official Capacity Defendants”) move to dismiss the claims brought against them by Plaintiffs Xiaoxing Xi, Qi Li, and Joyce Xi on the grounds that this Court lacks jurisdiction over those claims, and that they fail to state a claim upon which relief may be granted. The grounds for this motion are set forth more fully in the accompanying memorandum in support of this motion. A proposed order is attached.

Dated: February 2, 2018

Respectfully submitted,

CHAD A. READLER  
Acting Assistant Attorney General  
Civil Division

ANTHONY J. COPPOLINO  
Deputy Director  
Civil Division, Federal Programs Branch

/s/ Elizabeth Tulis  
ELIZABETH TULIS  
(NY Bar, under LCvR 83.5(e))  
Trial Attorney  
United States Department of Justice  
Civil Division, Federal Programs Branch  
P.O. Box 883  
Washington, D.C. 20044  
(202) 514-9237 (phone)  
(202) 616-8470 (fax)  
E-mail: elizabeth.tulis@usdoj.gov

*Attorneys for Defendants Christopher A.  
Wray, Jefferson B. Sessions, III, and Adm.  
Michael S. Rogers*

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

XIAOXING XI, *et al.*,

Plaintiffs,

v.

Civil Action No. 17-2132

FBI SPECIAL AGENT ANDREW  
HAUGEN, *et al.*,

Defendants.

**MEMORANDUM IN SUPPORT OF THE GOVERNMENT'S  
MOTION TO DISMISS PLAINTIFFS' CLAIMS AGAINST OFFICIAL  
CAPACITY DEFENDANTS CHRISTOPHER A. WRAY, JEFFERSON B.  
SESSIONS, III, AND ADM. MICHAEL S. ROGERS**

CHAD A. READLER  
Acting Assistant Attorney General  
Civil Division

ANTHONY J. COPPOLINO  
Deputy Director  
Civil Division, Federal Programs Branch

ELIZABETH TULIS  
(NY Bar, under LCvR 83.5(e))  
Trial Attorney  
United States Department of Justice  
Civil Division, Federal Programs Branch  
P.O. Box 883  
Washington, D.C. 20044  
(202) 514-9237 (phone)  
(202) 616-8470 (fax)  
E-mail: elizabeth.tulis@usdoj.gov

## TABLE OF CONTENTS

	PAGE
INTRODUCTION .....	1
BACKGROUND .....	3
A.    The Underlying Criminal Case .....	3
B.    The Instant Lawsuit.....	4
C.    Foreign Intelligence Surveillance Authorities Referenced in Plaintiffs’ Second Amended Complaint .....	6
1.    Traditional FISA .....	6
2.    FISA Section 702.....	7
3.    Executive Order 12,333 .....	12
ARGUMENT.....	13
I.    Plaintiffs’ Claims Should Be Dismissed for Lack of Subject Matter Jurisdiction .....	13
A.    Legal Standards.....	13
B.    Plaintiffs Lack Standing to Seek an Expungement Remedy .....	15
C.    Plaintiffs Lack Standing to Seek a Declaratory Judgment.....	18
II.   Plaintiffs’ Claims Should Be Dismissed for Failure to State a Claim Upon Which Relief May Be Granted.....	20
A.    Legal Standards.....	20
B.    Plaintiffs Do Not Plausibly Allege that They Were Subjected to Searches or Seizures Conducted Pursuant to Search Warrants or FISA Orders Issued Without Probable Cause .....	21
C.    Xi Does Not Plausibly Allege that the Government Violated His Fourth Amendment Rights Through Warrantless Surveillance Under FISA Section 702 or EO 12,333 .....	24

1.	Xi Does Not Plausibly Allege that His Fourth Amendment Rights Were Violated by Warrantless Surveillance Under FISA Section 702.....	24
a.	Xi Does Not Plausibly Allege that His Communications Were Intercepted Through Surveillance Under Section 702.....	25
b.	Xi Does Not Plausibly Allege that Any Purported Section 702 Surveillance Violated the Fourth Amendment .....	27
2.	Xi Does Not Plausibly Allege that the Government Violated His Fourth Amendment Rights by Conducting Surveillance Under EO 12,333 .....	34
3.	Xi Does Not Plausibly Allege that the Government Violated His Fourth Amendment Rights by Querying Databases Containing Information Collected Pursuant to Section 702 or EO 12,333 .....	37
	CONCLUSION.....	38

## TABLE OF AUTHORITIES

CASES	PAGE(S)
<i>Already, LLC v. Nike, Inc.</i> , 568 U.S. 85 (2013).....	14
<i>Anderson v. Holder</i> , 673 F.3d 1089 (9th Cir. 2012) .....	6
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	<i>passim</i>
<i>Bd. of Educ. Indep. Sch. Dist. No. 92 of Pottawatomie Cty. v. Earls</i> , 536 U.S. 822 (2002).....	33
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007).....	20
<i>Bey v. Genano</i> , No. PWG-16-2800, 2017 WL 1315530 (D. Md. Apr. 10, 2017).....	23
<i>Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics</i> , 403 U.S. 388 (1971).....	4
<i>Brown v. Fauver</i> , 819 F.2d 395 (3d Cir. 1987).....	14
<i>Brown v. Muhlenberg Twp.</i> , 269 F.3d 205 (3d Cir. 2001).....	16
<i>Buck v. Hampton Twp. Sch. Dist.</i> , 452 F.3d 256 (3d Cir. 2006).....	3
<i>Cassidy v. Chertoff</i> , 471 F.3d 67 (2d Cir. 2006).....	30
<i>City of Indianapolis v. Edmond</i> , 531 U.S. 32 (2000).....	28
<i>City of Los Angeles v. Lyons</i> , 461 U.S. 95 (1983).....	14, 18, 19
<i>Clapper v. Amnesty Int’l USA</i> , 133 S. Ct. 1138 (2013).....	<i>passim</i>

<i>DaimlerChrysler Corp. v. Cuno</i> , 547 U.S. 332 (2006).....	13, 14
<i>Danvers Motor Co. v. Ford Motor Co.</i> , 432 F.3d 286 (3d Cir. 2005).....	13, 14
<i>In re Directives Pursuant to Section 105B of FISA</i> , 551 F.3d 1004 (FISC Ct. Rev. 2008).....	<i>passim</i>
<i>Eaton v. Tosti</i> , No. CIV.09-5248 (WJM), 2010 WL 2483318 (D.N.J. June 4, 2010) .....	22
<i>Fed. Election Comm’n v. Hall-Tyner Election Campaign Comm.</i> , 524 F. Supp. 955 (S.D.N.Y. 1981), <i>aff’d</i> , 678 F.2d 416 (2d Cir. 1982) .....	6
<i>Franks v. Delaware</i> , 438 U.S. 154 (1978).....	22, 23
<i>Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.</i> , 528 U.S. 167 (2000).....	14
<i>Gould Elec., Inc. v. United States</i> , 220 F.3d 169 (3d Cir. 2000).....	14
<i>Griffin v. Wisconsin</i> , 483 U.S. 868 (1987).....	28
<i>In re Horizon Healthcare Servs. Inc. Data Breach Litig.</i> , 846 F.3d 625 (3d Cir. 2017).....	14
<i>INS v. Lopez-Mendoza</i> , 468 U.S. 1032 (1984).....	20
<i>J. Roderick MacArthur Found. v. F.B.I.</i> , 102 F.3d 600 (D.C. Cir. 1996).....	18
<i>Kerchner v. Obama</i> , 612 F.3d 204 (3d Cir. 2010).....	13
<i>Laird v. Tatum</i> , 408 U.S. 1, (1972).....	17, 19
<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992).....	13, 14, 17, 20

<i>Maryland v. King</i> , 133 S. Ct. 1958 (2013).....	31, 32
<i>Mayfield v. United States</i> , 599 F.3d 964 (9th Cir. 2010) .....	19
<i>Messerschmidt v. Millender</i> , 565 U.S. 535 (2012).....	21
<i>Mohamud v. United States</i> , No. 17-5126, --- S.Ct. ----, 2018 WL 311442 (Jan. 18, 2018).....	29
<i>Moore v. City of New York</i> , No. 08-CV-2449 RRM LB, 2011 WL 795103 (E.D.N.Y. Feb. 28, 2011) .....	23
<i>Naranjo v. City of Philadelphia</i> , 626 F. App'x 353 (3d Cir. 2015) .....	18
<i>Nat'l Treasury Emps. Union v. Von Raab</i> , 489 U.S. 656 (1989).....	28
<i>New Jersey v. T.L.O.</i> , 469 U.S. 325 (1985).....	28
<i>Overfield v. Pennroad Corp.</i> , 146 F.2d 889 (3d Cir. 1944).....	6
<i>Paton v. La Prade</i> , 524 F.2d 862 (3d Cir. 1975).....	17, 18
<i>Pennsylvania Bd. of Probation &amp; Parole v. Scott</i> , 524 U.S. 357 (1998).....	20
<i>Pennsylvania v. Mimms</i> , 434 U.S. 106 (1977).....	27
<i>Raines v. Byrd</i> , 521 U.S. 811 (1997).....	13
[Redacted Caption], 2011 WL 10945618 (FISA Ct. Oct. 3, 2011) .....	29, 30, 32
<i>Rumely v. United States</i> , 197 F.2d 166 (D.C. Cir. 1952).....	6



<i>Samson v. California</i> , 547 U.S. 843 (2006).....	31
<i>Schuchardt v. President of the United States</i> , 839 F.3d 336 (3d Cir. 2016).....	26, 27
<i>In re Schering Plough Corp. Intron/Temodar Consumer Class Action</i> , 678 F.3d 235 (3d Cir. 2012).....	13
<i>In re Sealed Case</i> , 310 F.3d 717 (FISC Ct. Rev. 2002).....	30, 33
<i>In re Search Warrant No. 16-960-M-01 to Google</i> , 232 F. Supp. 3d 708 (E.D. Pa. 2017) .....	16
<i>In re Search Warrant No. 16-960-M-01 to Google</i> , MJ No. 16-1061, 2017 WL 3535037 (E.D. Pa. Aug. 17, 2017) .....	16
<i>In re Search Warrant To Google, Inc.</i> , Mag. No. 16-4116, 2017 WL 2985391 (D.N.J. July 10, 2017) .....	16
<i>Segura v. United States</i> , 468 U.S. 796 (1984).....	15
<i>Sheare v. Borough of Olyphant</i> , No. 3:11-CV-1639, 2012 WL 140233 (M.D. Pa. Jan. 18, 2012).....	24
<i>Terry v. Ohio</i> , 392 U.S. 1 (1968).....	27
<i>United States v. Abu-Jihaad</i> , 630 F.3d 102 (2d Cir. 2010).....	22
<i>United States v. Aziz</i> , 228 F. Supp. 3d 363 (M.D. Pa. 2017).....	22
<i>United States v. Butenko</i> , 494 F.2d 593 (3d Cir. 1974).....	28, 29
<i>United States v. Calandra</i> , 414 U.S. 338 (1974).....	<i>passim</i>
<i>United States v. Cavanagh</i> , 807 F.2d 787 (9th Cir. 1987) .....	22

<i>United States v. Damrah</i> , 412 F.3d 618 (6th Cir. 2005) .....	22
<i>United States v. Duka</i> , 671 F.3d 329 (3d Cir. 2011).....	22, 28, 29
<i>United States v. Figueroa</i> , 757 F.2d 466 (2d Cir. 1985).....	32
<i>United States v. Hasbajrami</i> , No. 11-cr-623 (JG), 2016 WL 1029500 (E.D.N.Y. Mar. 8, 2016) .....	31, 33
<i>United States v. Huang</i> , 15 F. Supp. 3d 1131 (D.N.M. 2014) .....	23
<i>United States v. Jacobsen</i> , 466 U.S. 109 (1984).....	15, 16, 38
<i>United States v. Johnson</i> , 952 F.2d 565 (1st Cir. 1991).....	22
<i>United States v. Leon</i> , 468 U.S. 897 (1984).....	21
<i>United States v. Mohamud</i> , No. 3:10–CR–00475–KI–1, 2014 WL 2866749 (D. Or. June 24, 2014) <i>aff’d</i> , 843 F.3d 420 (9th Cir. 2016) .....	<i>passim</i>
<i>United States v. Mubayyid</i> , 521 F. Supp. 2d 125 (D. Mass. 2007) .....	23
<i>United States v. Muhtorov</i> , 187 F. Supp. 3d 1240 (D. Colo. 2015).....	31, 33
<i>United States v. Ning Wen</i> , 477 F.3d 896 (7th Cir. 2007) .....	22
<i>United States v. Pelton</i> , 835 F.2d 1067 (4th Cir. 1987) .....	22
<i>United States v. Truong Dinh Hung</i> , 629 F.2d 908 (4th Cir. 1980) .....	28, 29, 30
<i>United States v. U.S. Dist. Court (Keith)</i> , 407 U.S. 297 (1972).....	28, 29

<i>United States v. Verdugo–Urquidez</i> , 494 U.S. 259 (1990).....	31
<i>United States v. Yusuf</i> , 461 F.3d 374 (3d Cir. 2006).....	21, 22, 23
<i>United States v. Zakharov</i> , 468 F.3d 1171 (9th Cir. 2006) .....	31
<i>Valley Forge Christian Coll. v. Ams. United for Separation of Church &amp; States</i> , 454 U.S. 464 (1982).....	13
<i>Wag-Aero, Inc. v. United States</i> , 837 F. Supp. 1479 (E.D. Wis. 1993), <i>aff’d</i> , 35 F.3d 569 (7th Cir. 1994) .....	23
<i>Warth v. Seldin</i> , 422 U.S. 490 (1975).....	13

## STATUTES

28 U.S.C. § 1346(b)(1) .....	4
28 U.S.C. § 2671-2680 .....	4
50 U.S.C. § 1801 <i>et seq.</i> .....	6
50 U.S.C. § 1801-1812 .....	3, 25
50 U.S.C. § 1801(f).....	6, 8
50 U.S.C. § 1801(f)(2) .....	8
50 U.S.C. § 1801(h) .....	7
50 U.S.C. § 1803.....	6
50 U.S.C. § 1804(a) .....	6
50 U.S.C. § 1805.....	6
50 U.S.C. § 1805(a)(2).....	6
50 U.S.C. § 1805(a)(3).....	7
50 U.S.C. § 1805(c)(2)(A) .....	7
50 U.S.C. § 1821-1829 .....	3, 25
50 U.S.C. § 1821(4) .....	7
50 U.S.C. § 1821(5) .....	6
50 U.S.C. § 1823(a) .....	6
50 U.S.C. § 1824.....	6
50 U.S.C. § 1824(a)(2).....	7
50 U.S.C. § 1824(a)(3).....	7
50 U.S.C. § 1824(c)(2)(A) .....	7
50 U.S.C. § 1881a.....	4, 9, 25
50 U.S.C. § 1881a(a).....	9
50 U.S.C. § 1881a(b) .....	10
50 U.S.C. § 1881a(b)(5).....	10
50 U.S.C. § 1881a(c)(1).....	32

50 U.S.C. § 1881a(e).....	32
50 U.S.C. § 1881a(g) .....	9
50 U.S.C. § 1881a(g)(1).....	33
50 U.S.C. § 1881a(g)(2)(A)(v) .....	29
50 U.S.C. § 1881a(g)(2)(A)(vi) .....	10
50 U.S.C. § 1881a(h)(1).....	10
50 U.S.C. § 1881a(i)(2)(B) .....	33

Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, 108 Stat. 3423 (Oct. 14, 1994) .....	6
FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (July 10, 2008) .....	9
FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, 132 Stat. 3 (Jan. 19, 2018) .....	9

## **EXECUTIVE ORDERS**

EO 12,333, 46 Fed. Reg. 59941 (December 4, 1981).....	<i>passim</i>
EO 13,284, 68 Fed. Reg. 4075 (Jan. 23, 2003) .....	12
EO 13,355, 69 Fed. Reg. 53593 (Aug. 27, 2004) .....	12
EO 13,470, 73 Fed. Reg. 45325 (July 30, 2008) .....	12

## **LEGISLATIVE MATERIALS**

Modernization of the FISA: Hearing before the S. Select Comm. On Intel., 110th Cong., 1st Sess. (2007) .....	8, 9
S. Rep. No. 95-604 (1977) .....	6
S. Rep. No. 95-701 (1978) .....	8
S. Rep. No. 110-209 (2007) .....	8

## **FEDERAL RULES OF CIVIL PROCEDURE**

Rule 12(b)(1).....	2, 14, 27, 38
Rule 12(b)(6).....	<i>passim</i>

## INTRODUCTION

The Court should dismiss the claims asserted in Count X of Plaintiffs' second amended complaint for lack of subject matter jurisdiction and failure to state a claim upon which relief may be granted. Styled as a Fourth Amendment claim, Count X alleges that the Department of Justice ("DOJ"), the National Security Agency ("NSA"), and the Federal Bureau of Investigation ("FBI") (collectively, "the Official Capacity Defendants" or "the Government"), through defendant Andrew Haugen and other "agents," conducted illegal searches and seizures, and that the Government continues to retain information acquired through these alleged searches and seizures. On the basis of these allegations, Plaintiffs seek an injunction requiring the Government to expunge any information obtained through the alleged searches and seizures and a declaration that the Government violated their Fourth Amendment rights.

As a threshold matter, Plaintiffs lack Article III standing to bring these claims. Plaintiffs do not allege any concrete injury stemming from the Government's alleged retention of information obtained through the alleged searches or seizures. They therefore have not alleged any injury in fact that would give them standing to seek expungement of the information. Further, Plaintiffs do not plausibly allege that they are subject to any ongoing or imminent future unlawful searches or seizures, and the declaratory judgment they seek thus would not redress their alleged Fourth Amendment injury. Nor would a declaratory judgment compel the Government to return or expunge information acquired through those searches and seizures, even if Plaintiffs had alleged some other cognizable Article III injury stemming from the Government's alleged retention of the information.

Accordingly, their claims against the Official Capacity Defendants should be dismissed for lack of jurisdiction.

The claims against the Official Capacity Defendants also fail on the merits, as Plaintiffs do not plausibly allege a violation of their Fourth Amendment rights. Plaintiffs allege that the Government violated their Fourth Amendment rights by (1) conducting searches and seizures based on search warrants and Foreign Intelligence Surveillance Act (“FISA”) orders issued without probable cause on the basis of false affidavits or applications, and (2) intercepting Plaintiff Xiaoxing Xi’s communications through warrantless surveillance conducted under the authority of FISA Section 702 “and/or” Executive Order (“EO”) 12,333. With respect to the first theory, Plaintiffs’ conclusory allegations that warrants and FISA orders were issued on the basis of unspecified false statements are insufficient to state a Fourth Amendment claim. And the second theory—that Xi’s communications were unlawfully obtained through warrantless surveillance under Section 702 “and/or” EO 12,333—is unsupported by any allegations supporting a plausible inference that such surveillance even occurred. Moreover, even if Xi plausibly alleged that his communications were collected through surveillance under Section 702 or EO 12,333, he has not plausibly alleged that the surveillance constituted an unreasonable search or seizure in violation of the Fourth Amendment. He also has not plausibly alleged any Fourth Amendment violation based on alleged querying of databases containing information collected through alleged surveillance under Section 702 or EO 12,333.

Accordingly, the claims against the Official Capacity Defendants should be dismissed pursuant to Rule 12(b)(1) and Rule 12(b)(6) of the Federal Rules of Civil Procedure.

## BACKGROUND<sup>1</sup>

### A. The Underlying Criminal Case

On or about May 14, 2015, a grand jury in the Eastern District of Pennsylvania returned an Indictment charging plaintiff Xiaoxing Xi (“Xi”) with four counts of wire fraud. ECF No. 24-1, Second Amended Complaint (“Second Am. Compl.”) ¶ 24; Indictment, *United States v. Xi*, 2:15-cr-00204-RBS (E.D. Pa. May 14, 2015), ECF No. 1.

On May 21, 2015, Xi was arrested at his home. Second Am. Compl. ¶¶ 32-33. That day, Plaintiffs’ home was searched pursuant to a search warrant, leading to the seizure of certain property belonging to Plaintiffs, including electronic devices, travel records, financial records, and other records of business and personal activities. *Id.* ¶ 67.

On June 5, 2015, Xi was arraigned before a magistrate judge. Minute Entry, *United States v. Xi*, 2:15-cr-00204-RBS (E.D. Pa. June 5, 2015), ECF No. 13. On June 9, 2015, the Government provided a “Notice of Intent to Use Foreign Intelligence Surveillance Information” in the criminal proceedings. *See* Notice of Intent to Use FISA Information, *United States v. Xi*, 2:15-cr-00204-RBS (E.D. Pa. June 9, 2015), ECF No. 16 (“FISA Notice”). Specifically, the Government provided notice that:

pursuant to Title 50, United States Code, Sections 1806(c) and 1825(d), the United States intends to offer into evidence, or otherwise use or disclose in any proceedings in the above-captioned matter, information obtained or derived from electronic surveillance and physical search conducted pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended, 50 U.S.C. §§ 1801-1812 and 1821-1829.

---

<sup>1</sup> The facts below are taken from the well-pleaded allegations in Plaintiffs’ Second Amended Complaint, documents incorporated by reference in the complaint, and items of which judicial notice may be taken. *See Buck v. Hampton Twp. Sch. Dist.*, 452 F.3d 256, 260 (3d Cir. 2006). For the purposes of this motion to dismiss only, the Court may assume the veracity of the well-pleaded factual allegations in the complaint. *See Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009).

*Id.* The Notice did not state that the Government intended to use any information obtained or derived from electronic surveillance conducted pursuant to FISA Section 702, 50 U.S.C. § 1881a. *See* FISA Notice.

On September 18, 2015, the indictment was dismissed on the Government's motion. Second Am. Compl. ¶ 52; Order, *United States v. Xi*, 2:15-cr-00204-RBS (E.D. Pa. Sept. 18, 2015), ECF No. 30.

### **B. The Instant Lawsuit**

Xi first filed a complaint naming Special Agent Haugen as the sole defendant, and alleging five claims against him under *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971). Four counts were for alleged violations of Xi's Fourth Amendment rights in the course of (1) the prosecution of Xi; (2) purported surveillance of Xi pursuant to "FISA orders"; (3) alleged warrantless surveillance of Xi pursuant to Section 702 of FISA; and (4) the search of Xi and his belongings following his arrest. One count was for alleged violation of Xi's equal protection and due process rights under the Fifth Amendment in the course of Xi's indictment and prosecution. *See* Compl., ECF No. 1, ¶¶ 72-82. Xi also sought an injunction "requiring" Special Agent Haugen to return or destroy all information obtained from Xi's electronic communications and devices that is in his custody or control. *Id.* at 20.

Xi then amended his complaint, adding six claims against the United States under the Federal Tort Claims Act, 28 U.S.C. §§ 1346(b)(1), 2671-2680 (2012) (FTCA), and adding his wife and daughter as plaintiffs on the FTCA claims only. *See* Am. Compl., ECF No. 6-1. Special Agent Haugen and the United States each filed dispositive motions to



dismiss the respective claims against them. *See* United States’ Motion to Dismiss, ECF No. 15; Haugen’s Motion to Dismiss, ECF No. 16.

Plaintiffs then amended their complaint a second time, dropping the Fourth Amendment claims against Special Agent Haugen for the alleged surveillance of Xi under “FISA orders” and the purported warrantless surveillance of Xi under Section 702 of FISA, *see generally* Second Am. Compl., and adding putative Fourth Amendment claims against the Official Capacity Defendants based on alleged illegal physical searches and electronic surveillance, *id.* ¶ 124. Specifically, Plaintiffs claim that their Fourth Amendment rights were violated based on allegations that (1) the “FBI, DOJ, and/or NSA” caused physical searches and seizures of their property and interception of their electronic communications pursuant to search warrants and FISA orders issued without probable cause on the basis of false statements, *id.* ¶¶ 125-130, (2) the “FBI, DOJ, and/or NSA” caused the interception of Xi’s communications “without obtaining a warrant” and “without notice,” *id.* ¶¶ 131-32, and (3) the Government continues to retain copies of information obtained through or derived from these alleged searches and seizures, Second Am. Compl. ¶¶ 133-35. Plaintiffs claim that they are therefore entitled to an injunction requiring the Official Capacity Defendants to return or expunge “all information in their custody or control obtained from [P]laintiffs’ electronic devices, communications, and papers” and a declaration that the Official Capacity Defendants violated their rights “by subjecting [them] to unlawful searches and seizures.” *Id.* at 34.

## C. Foreign Intelligence Surveillance Authorities Referenced in Plaintiffs’ Second Amended Complaint

### 1. Traditional FISA

In 1978 Congress enacted the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.* (“FISA”) “to regulate the use of electronic surveillance within the United States for foreign intelligence purposes,” S. Rep. No. 95-604, at 7 (1977),<sup>2</sup> placing certain types of foreign-intelligence surveillance under the oversight of the Foreign Intelligence Surveillance Court (“FISC”), *see* 50 U.S.C. § 1803. The statute was amended in 1994 to include parallel provisions governing physical searches. *See* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. 103-359, 108 Stat. 3423 (Oct. 14, 1994). Before the Government may conduct “electronic surveillance” or a “physical search” (as defined in FISA) to obtain foreign-intelligence information, the statute generally requires the Government to obtain an order from a FISC judge. *See* 50 U.S.C. §§ 1801(f), 1804(a), 1805, 1821(5), 1823(a), 1824.

To obtain such an order for electronic surveillance, the Government must show “probable cause to believe that . . . the [surveillance] target . . . is a foreign power or an agent of a foreign power,” and that “each of the facilities or places at which the surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power.” *Id.* § 1805(a)(2). The Government must also establish that it will employ

---

<sup>2</sup> “Courts can and do take judicial notice of such Congressional proceedings.” *Overfield v. Pennroad Corp.*, 146 F.2d 889, 898 (3d Cir. 1944); *see also Anderson v. Holder*, 673 F.3d 1089, 1094 n.1 (9th Cir. 2012) (“Legislative history is properly a subject of judicial notice.”); *Rumely v. United States*, 197 F.2d 166, 181 (D.C. Cir. 1952) (noting that “judicial notice can be taken of congressional hearings”); *Fed. Election Comm’n v. Hall-Tyner Election Campaign Comm.*, 524 F. Supp. 955, 959 n.7 (S.D.N.Y. 1981) (taking judicial notice of Senate Report), *aff’d*, 678 F.2d 416 (2d Cir. 1982).

“minimization procedures” that are “reasonably designed in light of the purpose and technique of the particular surveillance[ ] to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.” *Id.* § 1801(h); *see also id.* § 1805(a)(3), (c)(2)(A).

Likewise, to obtain such an order for a physical search, the Government must show “probable cause to believe that . . . the target of the physical search is a foreign power or an agent of a foreign power,” and that “the premises or property to be searched is or is about to be owned, used, possessed by, or in transit to or from an agent of a foreign power or a foreign power.” *Id.* § 1824(a)(2). The Government must again also establish that it will employ “minimization procedures” that are “reasonably designed in light of the purposes and technique of the particular physical search, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.” *Id.* § 1821(4); *see also id.* § 1824(a)(3), (c)(2)(A).

## **2. FISA Section 702**

In 2008, Congress amended FISA and enacted Section 702, which authorized the collection of electronic communications of non-U.S. persons located outside the United States. *See* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*

(“PCLOB Report”) at 5, 6 (July 2, 2014).<sup>3</sup> These revisions were enacted to modernize FISA in the wake of changes in communications technology. By way of background, when Congress originally enacted FISA, it focused on foreign-intelligence surveillance of persons within the United States, by limiting the definition of “electronic surveillance,” to which FISA’s requirements are keyed, to domestically targeted foreign-intelligence-collection activities. *Id.* § 1801(f). Congress intentionally excluded from FISA the vast majority of Government surveillance then conducted outside the United States, even if it targeted U.S. persons abroad or incidentally acquired, while targeting other parties abroad, communications to or from U.S. persons or persons located in the United States. *See S. Rep. No. 95-701*, at 7, 34-35, 71 (1978).

In 2006, Congress began considering amendments to modernize FISA because of changes in communications technology. *See S. Rep. No. 110-209*, at 2-5 (2007); *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138, 1143-44 (2013). Whereas international communications were predominantly carried by radio or satellite when FISA was enacted, they were now predominantly carried by fiber optic cables, and so qualified as wire communications subject to FISA’s requirements. *See Modernization of the FISA: Hearing before the S. Select Comm. On Intel.*, 110th Cong., 1st Sess., at 18-19 (2007) (“May 1, 2007 FISA Mod. Hrg.”). Further, FISA’s “electronic surveillance” definition “place[d] a premium on the location of the collection”: intercepts of wire or other non-radio communications conducted inside the United States were covered, while those conducted outside the U.S. generally were not. *Id.* at 19; 50 U.S.C. § 1801(f)(2). The global integration

---

<sup>3</sup> The PCLOB Report is incorporated by reference in paragraph 64, footnote 3 of Plaintiffs’ Complaint.

of communications technology had rendered this distinction outmoded too. *See* May 1, 2007 FISA Mod. Hrg. at 19 (“Today, a single communication can transit the world even if the two people communicating are only located a few miles apart.”). Due to these technological changes, the Government had to expend significant resources to craft FISA applications for surveillance that was originally intended to be outside FISA’s scope. *Id.* at 18; *see* PCLOB Report at 20-24.

Congress addressed this problem through enactment of the FISA Amendments Act of 2008 (“FAA”), Pub. L. No. 110-261. Section 702 of FISA, 50 U.S.C. § 1881a,<sup>4</sup> “supplements pre-existing FISA authority by creating a new framework under which the Government may seek the FISC’s authorization of certain foreign intelligence surveillance targeting . . . non-U.S. persons located abroad,” *Amnesty Int’l*, 133 S. Ct. at 1144, without regard to the means by which the targeted communications are transmitted or where they are intercepted. Section 702 generally provides that, upon FISC approval of a “certification” submitted by the Government, and of targeting and minimization procedures, the Attorney General and the Director of National Intelligence (“DNI”) may jointly authorize, for up to one year, the “targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.” 50 U.S.C. § 1881a(a), (g); PCLOB Report at 20-24. The Government must acquire the information from or with the assistance of an electronic communications service provider, to which end the Attorney General and the DNI may issue “directives” to providers compelling their

---

<sup>4</sup> In 2018, Congress amended Section 702, which resulted, *inter alia*, in the re-numbering of some sections cited in this memorandum. *See* FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, 132 Stat. 3 (Jan. 19, 2018). All citations herein are to the prior version of the statute, i.e., the version of 50 U.S.C. § 1881a in effect as of the date of the filing of Plaintiffs’ complaint in 2017.

assistance in the acquisition of the targeted communications. 50 U.S.C. § 1881a(g)(2)(A)(vi), (h)(1); PCLOB Report at 21-22. Under the express terms of Section 702, the Government cannot intentionally target a U.S. person overseas or persons (including U.S. persons) known at the time of acquisition to be in the United States. 50 U.S.C. § 1881a(b). The acquisition must also be “conducted in a manner consistent with the [F]ourth [A]mendment.” *Id.* § 1881a(b)(5).

Pursuant to Section 702 certifications, communications are acquired with the compelled assistance of electronic communications service providers through the “tasking” (i.e. designation) of “selectors.” PCLOB Report at 32-33. “A selector must be a specific communications facility that is assessed to be used by the target, such as the target’s email address or telephone number.” *Id.* at 32. Accordingly, only selectors used by non-U.S. persons reasonably believed to be located abroad may be tasked. *Id.* at 33.

Prior to tasking a selector, NSA analysts must follow FISC-approved targeting procedures to ensure that they are targeting a non-U.S. person reasonably believed to be located outside the United States, who possesses or is likely to receive or communicate foreign intelligence information authorized for acquisition. *Id.* at 42-48. Analysts must also assess whether tasking the particular selector will be likely to acquire foreign intelligence information. *Id.* at 45. These determinations then must undergo internal NSA review. *Id.* at 46.

Once a selector has been tasked under the targeting procedures, it is sent to an electronic communications service provider to begin acquisition, of which there are two types: “PRISM” collection and “Upstream” collection. *Id.* at 33-41.

According to the PCLOB Report incorporated by reference in Plaintiffs' Second Amended Complaint:

In PRISM collection, the Government sends a selector to a United States-based electronic communications service provider, such as an Internet service provider, that has been served a directive that compels the service provider to provide the Government with communications sent to or from the selector. *Id.* at 33. The acquisition of communications of a particular selector continues until the Government “detasks” the selector. *Id.* at 34. The NSA receives all PRISM collection, and a copy of the raw data acquired via PRISM collection may also be sent to the CIA and/or FBI. *Id.* The NSA, CIA, and FBI all must apply their own minimization procedures to any PRISM-acquired data. *Id.*

In Upstream collection, tasked selectors are sent to a U.S. electronic communications service provider to acquire communications that are transiting the “Internet backbone,” i.e., the “circuits that are used to facilitate Internet communications.” *Id.* at 36-37. This process involves filtering Internet transactions to eliminate potential domestic transactions, and then screening the transactions to capture only those containing a tasked selector. *Id.* at 37. “Unless [communications] pass both these screens, they are not ingested into Government databases.” *Id.* Raw Upstream data resides only with NSA—the FBI and CIA do not receive a copy of unminimized data acquired via Upstream collection. *Id.* at 35. The NSA is not permitted to use U.S.-person identifiers in querying Upstream data. *Id.* at 85.

Both PRISM and Upstream collection thus are targeted forms of acquisition aimed at capturing communications associated with approved selectors, not methods of bulk

collection in which communications data are collected on a large scale without the use of specified selectors. *Id.* at 111-12.

Unminimized data acquired under Section 702 generally must be aged off of the NSA, CIA, and FBI systems no later than five years after the expiration of the Section 702 certification under which the data was acquired. *Id.* at 60.<sup>5</sup> However, unminimized internet transactions acquired via Upstream collection—which are never provided to the FBI or CIA—“must be aged off the NSA systems no later than two years after the expiration of the [relevant] Section 702 certification.” *Id.*

### **3. Executive Order 12,333**

The Government also has authority to conduct foreign intelligence surveillance outside of the United States against non-U.S. persons under EO 12,333, which was issued by President Reagan in 1981. EO 12,333, 46 Fed. Reg. 59941(December 4, 1981), amended by EO 13,284, 68 Fed. Reg. 4075 (Jan. 23, 2003), EO 13,355, 69 Fed. Reg. 53593 (Aug. 27, 2004), and EO 13,470, 73 Fed. Reg. 45325 (July 30, 2008)); *see* PCLOB Report at 107. The order, which has been amended three times, authorizes the NSA to, *inter alia*, “[c]ollect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions,” and “for the conduct of military operations.” EO 12,333, § 1.7(c)(1), (5). It also provides, *inter alia*, that intelligence elements of the FBI shall “[c]ollect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support

---

<sup>5</sup> “Minimized” data refers to data that has been evaluated and determined to either contain no U.S. person information or only U.S. person information that meets the standard for permanent retention. PCLOB Report at 60.



national and departmental missions, in accordance with procedural guidelines approved by the Attorney General, after consultation with the Director.” *Id.* § 1.7(g)(1). The order expressly provides that nothing in it “shall be construed to authorize any activity in violation of the Constitution or statutes of the United States.” *Id.* § 2.8.

## ARGUMENT

### I. Plaintiffs’ Claims Should Be Dismissed for Lack of Subject Matter Jurisdiction.

#### A. Legal Standards

“[T]he ‘judicial power’ of the United States” is limited by Article III of the Constitution “to the resolution of ‘cases’ and ‘controversies.’” *Valley Forge Christian Coll. v. Ams. United for Separation of Church & States*, 454 U.S. 464, 471 (1982); *see DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 341 (2006); *In re Schering Plough Corp. Intron/Temodar Consumer Class Action*, 678 F.3d 235, 244 (3d Cir. 2012). A plaintiff’s standing to sue “is an essential and unchanging part of the case-or-controversy requirement,” *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992), without which the court lacks jurisdiction to entertain the suit. *Warth v. Seldin*, 422 U.S. 490, 498 (1975); *Kerchner v. Obama*, 612 F.3d 204, 207 (3d Cir. 2010). The Supreme Court “ha[s] always insisted on strict compliance with this jurisdictional standing requirement.” *Raines v. Byrd*, 521 U.S. 811, 819 (1997).

To establish Article III standing, a plaintiff must seek relief for an injury that is (1) “concrete, particularized, and actual or imminent”—i.e. an “injury in fact”; (2) “fairly traceable to the challenged action”; and (3) “redressable by a favorable ruling.” *Amnesy Int’l*, 133 S. Ct. at 1147 (citation omitted). The alleged injury must be “distinct and palpable,” not “abstract or conjectural or hypothetical.” *Danvers Motor Co. v. Ford Motor*

*Co.*, 432 F.3d 286, 291 (3d Cir. 2005). Speculative claims of injury will not support Article III standing. *Amnesty Int’l*, 133 S. Ct. at 1147. As the “party invoking federal jurisdiction,” a plaintiff “bears the burden of establishing these elements” of standing. *Defenders of Wildlife*, 504 U.S. at 561.

“[A] plaintiff must demonstrate standing separately for each form of relief sought.” *DaimlerChrysler Corp.*, 547 U.S. at 352; *see Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 185 (2000). “In order to obtain standing for prospective relief, the plaintiff must ‘establish a real and immediate threat that he would again be [the victim of the allegedly unconstitutional practice].’” *Brown v. Fauver*, 819 F.2d 395, 400 (3d Cir. 1987) (alteration in original) (quoting *City of Los Angeles v. Lyons*, 461 U.S. 95, 105 (1983)). Accordingly, a plaintiff is not entitled to declaratory or injunctive relief merely on the basis that he or she was injured by past unlawful conduct. *See, e.g., Already, LLC v. Nike, Inc.*, 568 U.S. 85, 98 (2013) (“[W]e have never held that a plaintiff has standing to pursue declaratory relief merely on the basis of being ‘once bitten.’ Quite the opposite.” (citing *Lyons*, 461 U.S. at 109)); *Lyons*, 461 U.S. at 105-07 (holding that plaintiff alleging that he had been injured by illegal police conduct had no standing to seek declaratory or injunctive relief because he had not made a sufficient showing that he was likely to be wronged again in a similar way).

“A Rule 12(b)(1) motion may be treated as either a facial or factual challenge to the court’s subject matter jurisdiction.” *Gould Elec., Inc. v. United States*, 220 F.3d 169, 176 (3d Cir. 2000). In reviewing a facial challenge to standing, the court “appl[ies] the same standard as on review of a motion to dismiss under Rule 12(b)(6).” *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 633 (3d Cir. 2017). Accordingly,

the court accepts the well-pleaded factual allegations of the complaint as true and draws all reasonable inferences in the plaintiff's favor. *Id.* "Nevertheless, '[t]hreadbare recitals of the elements of [standing], supported by mere conclusory statements, do not suffice.'" *Id.* (alterations in original) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)).

### **B. Plaintiffs Lack Standing to Seek an Expungement Remedy.**

Plaintiffs lack standing to seek an injunction requiring expungement of information allegedly obtained by the Government through unlawful searches and seizures because (1) such an injunction would not redress any Fourth Amendment injury suffered by Plaintiffs, and (2) Plaintiffs allege no concrete and particularized, actual or imminent injury stemming from the Government's alleged retention of the information that was allegedly unlawfully obtained.

First, the Government's mere retention of information obtained through an unlawful search or seizure does not violate the Fourth Amendment, and the injunction sought by Plaintiffs would not redress the searches and seizures that Plaintiffs contend were unlawful. The Fourth Amendment assures the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend IV, cl. 1. As the Supreme Court has explained, "[d]ifferent interests are implicated by a seizure than by a search. A seizure affects only [a] person's possessory interests; a search affects a person's privacy interests." *Segura v. United States*, 468 U.S. 796, 806 (1984) (citations omitted); see *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). To the extent Plaintiffs allege that their Fourth Amendment rights were violated by searches conducted without probable cause, Second Am. Compl. ¶¶ 83, 85, any such violation was "fully accomplished by the original search," *United States v. Calandra*, 414

U.S. 338, 354 (1974), and it would not be redressed by expungement of information obtained through the search.

Similarly, the injunction sought by Plaintiffs would not redress the alleged unlawful seizures of Plaintiffs' personal belongings, Second Am. Compl. ¶ 85, because Plaintiffs do not allege that the Government has failed to return any of these belongings or that they are being deprived of use of those belongings. Rather, Plaintiffs merely allege that the Government currently possesses "copies of the private data stored on [their] computers and other electronic devices." *Id.* ¶ 86. But the Government's alleged retention of such copies does not constitute a Fourth Amendment seizure because it does not cause any "meaningful interference with [Plaintiffs'] possessory interests in [their] property." *Jacobsen*, 466 U.S. at 113; accord *Brown v. Muhlenberg Twp.*, 269 F.3d 205, 209 (3d Cir. 2001); see, e.g., *In re Search Warrant No. 16-960-M-01 to Google*, 232 F. Supp. 3d 708, 720-21 (E.D. Pa. 2017), (holding that execution of search warrants that required the electronic transfer of data from a server in a foreign country to Google's data center in California would not result in a "seizure" in a foreign country, and noting that courts have held that photocopying documents, taking photographs of materials, and accessing electronic data are not "seizures" (collecting cases)), *aff'd sub nom. In re Search Warrant No. 16-960-M-1 to Google*, MJ No. 16-1061, 2017 WL 3535037 (E.D. Pa. Aug. 17, 2017); accord *In re Search Warrant To Google, Inc.*, Mag. No. 16-4116, 2017 WL 2985391, at \*10-11 (D.N.J. July 10, 2017).

Second, Plaintiffs allege no other concrete, particularized, and actual or imminent injury that stems from the Government's alleged retention of information acquired through the alleged unlawful searches and seizures. See Second Am. Compl. ¶¶ 83-86. Plaintiffs do

not allege that the Government is currently using information obtained through the alleged searches and seizures against Plaintiffs or that it will do so in the future. To the extent Plaintiffs allege a “fear” that any information currently in the Government’s possession may be “misused” at some future time, Second Am. Compl. ¶ 82,<sup>6</sup> any such professed “fear” is too speculative to constitute an injury in fact. *See, e.g., Laird v. Tatum*, 408 U.S. 1, 13, (1972) (rejecting argument that standing could be based on “speculative apprehensiveness that the Army may at some future date misuse the information [acquired through surveillance activities] in some way that would cause direct harm to respondents”). And the Government’s mere retention of such information does not by itself confer standing to seek an expungement remedy. *Compare Paton v. La Prade*, 524 F.2d 862, 868 (3d Cir. 1975) (distinguishing *Laird*, and finding that plaintiff demonstrated standing to seek expungement of FBI file that included a “Subversive Material-Socialist Workers Party” notation, because plaintiff plausibly alleged an injury resulting from retention of the file—specifically, that retention could endanger her future educational and employment opportunities).<sup>7</sup> Accordingly, Plaintiffs have not alleged any injury in fact that would

---

<sup>6</sup> In fact, Plaintiffs’ allegation regarding future misuse of information appears to be even more speculative: They assert that they are “in fear of *additional* illegal surveillance and other actions by the Government,” pointing to the now-dismissed indictment of Xi, and alleging that this past experience makes them “fear that their current and future words, phone calls, emails, and actions, however innocent, may be similarly misused by the Government.” Second Am. Compl. ¶ 82 (emphasis added). As discussed further below, Plaintiffs’ professed fear of future “illegal surveillance” is not a cognizable Article III injury. *See infra* at 18-19. But in any case, expungement of information currently in the Government’s possession would not redress hypothetical future misuse of other information that Plaintiffs speculate the Government might obtain.

<sup>7</sup> *Paton v. La Prade* was decided before the Supreme Court synthesized then existing case law in *Lujan v. Defenders of Wildlife* and explained that to support constitutional standing, an injury must be “concrete”, “particularized,” and “actual or imminent.” *Defenders of Wildlife*, 504 U.S. at 560. Under that standard, it is doubtful whether the risk to the plaintiff’s future educational and employment opportunities that the Third Circuit found

provide standing to seek an injunction requiring expungement of information acquired by the Government through the alleged searches and seizures.

### **C. Plaintiffs Lack Standing to Seek a Declaratory Judgment.**

Plaintiffs also lack standing to seek a declaration that the Government violated their Fourth Amendment rights “by subjecting [them] to unlawful searches and seizures,” Second Am. Compl. at 34, because they do not allege any cognizable Article III injury that would be redressed by such declaratory relief.

First, Plaintiffs do not identify any Fourth Amendment injury that would be redressed by a declaratory judgment. As the Supreme Court held in *City of Los Angeles v. Lyons*, 461 U.S. 95, a plaintiff may not seek prospective relief—whether a declaratory judgment or injunction—where the plaintiff alleges only past constitutional violations. Rather, a plaintiff’s standing to seek such relief depends “on whether he [is] likely to suffer future injury” from the same alleged conduct. *Id.* at 105. Here, although Plaintiffs claim that their Fourth Amendment rights were violated by certain past searches and seizures, Second Am. Compl. ¶¶ 59-60, 66, 83, 85, 124-131, they do not “allege facts from which it appears there is a substantial likelihood that [they] will suffer [such] injury in the future.” *Naranjo v. City of Philadelphia*, 626 F. App’x 353, 356 n.1 (3d Cir. 2015) (per curiam) (summary affirmance).

---

sufficient for standing in *Paton* would be concrete and imminent enough to constitute an injury in fact. *See, e.g., J. Roderick MacArthur Found. v. F.B.I.*, 102 F.3d 600, 606 (D.C. Cir. 1996) (finding that plaintiff did not demonstrate injury in fact stemming from FBI’s retention of records about it where affidavits “sp[oke] broadly of stigma and harm to the Foundation’s reputation” and “[a] ‘potential’ limitation upon employees’ future ‘employability’ lack[ed] concreteness” and immediacy). Here, in any case, even under the analysis of *Paton*, Plaintiffs do not plausibly allege any injury stemming from the mere retention of their information.

Speculation that Plaintiffs may be subject to unlawful searches or seizures in the future, Second Am. Compl. ¶ 82, does not cure this defect. While Plaintiffs assert that they “are in fear of additional illegal surveillance,” *id.*, such professed “fear” is not sufficient to establish an injury in fact or to circumvent their lack of standing to seek prospective relief for past injuries, as it does not establish a “real and immediate threat” that they will be subject to such future surveillance. *Lyons*, 461 U.S. at 105. *Cf. Amnesty Int’l*, 133 S. Ct. at 1151 (plaintiffs could not “manufacture” standing by making expenditures based on non-paranoid fear of hypothetical future surveillance); *Laird*, 408 U.S. at 13-14 (“Allegations of a subjective ‘chill’ are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm.”). Accordingly, any Fourth Amendment violation alleged by Plaintiffs would not be redressed by a declaratory judgment.

Second, Plaintiffs identify no other concrete and particularized, actual or imminent injury that would be redressed by a declaratory judgment. As explained above, *see supra* at 17, Plaintiffs’ allegation that the Government retains copies of their private data or information derived from illegal searches or seizures is not sufficient to establish injury in fact. But even if Plaintiffs alleged some cognizable Article III injury stemming from the Government’s alleged retention of copies of information obtained through alleged illegal searches or seizures, the declaratory judgment they seek would not redress that injury because it would not render the Government’s alleged possession of the information unlawful, and thus would not require the Government to return or expunge the materials. *See, e.g., Mayfield v. United States*, 599 F.3d 964, 971 (9th Cir. 2010) (holding that declaratory judgment would not redress alleged injury stemming from Government’s retention of materials acquired through allegedly unlawful FISA searches because the

Government would “not necessarily be required by a declaratory judgment to destroy or otherwise abandon the materials”).

Indeed, although the exclusionary rule ordinarily precludes the Government from introducing the fruits of an unconstitutional search or seizure as part of its case in chief in a criminal proceeding against the subject of the search, it does not foreclose the Government from making other uses of such evidence, let alone preclude the Government from retaining possession of the materials. *See Calandra*, 414 U.S. at 347-52 (noting that exclusionary rule “has never been interpreted to proscribe the use of illegally seized evidence”); *see, e.g., Pennsylvania Bd. of Probation & Parole v. Scott*, 524 U.S. 357, 362 (1998) (noting that the Supreme Court has continually declined to extend the exclusionary rule to proceedings other than criminal trials); *INS v. Lopez-Mendoza*, 468 U.S. 1032, 1034, 1050 (1984) (unlawfully obtained materials generally may be used against an alien in civil immigration proceedings). Accordingly, even if Plaintiffs alleged some concrete injury based on the Government’s alleged retention of information acquired through unconstitutional searches or seizures, it is not “likely, as opposed to merely speculative, that the [plaintiffs’] injury will be redressed” by the declaration they seek, *Defenders of Wildlife*, 504 U.S. at 561, and Plaintiffs therefore lack standing under Article III to seek a declaratory judgment.

## **II. Plaintiffs’ Claims Should Be Dismissed for Failure to State a Claim Upon Which Relief May Be Granted.**

### **A. Legal Standard**

To survive a Rule 12(b)(6) motion to dismiss, a complaint must allege “enough facts to state a claim [for] relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). The “facial plausibility” standard requires the plaintiff to allege



facts that add up to “more than a sheer possibility that a defendant has acted unlawfully.” *Iqbal*, 556 U.S. at 678-79. In reviewing a Rule 12(b)(6) motion, the court accepts as true all well pleaded facts in the complaint, but disregards legal conclusions and “[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements.” *Id.* at 678. While “[t]he plausibility standard is not akin to a ‘probability requirement,’” a plaintiff does not survive a Rule 12(b)(6) motion by pleading facts that are “merely consistent” with a defendant’s liability. *Id.* at 678. Rather, the factual allegations must “allow[ ] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.*

**B. Plaintiffs Do Not Plausibly Allege that They Were Subjected to Searches or Seizures Conducted Pursuant to Search Warrants or FISA Orders Issued Without Probable Cause.**

Plaintiffs fail to allege sufficient factual matter, accepted as true, to state a plausible claim that their home and Xi’s offices were searched pursuant to warrants issued without probable cause, Second Am. Compl. ¶¶ 125-27, or that they were subjected to searches or seizures conducted pursuant to FISA orders obtained without probable cause, *Id.* ¶¶ 125-30.

A search warrant is entitled to a “general presumption that an affidavit of probable cause supporting a search warrant is valid.” *United States v. Yusuf*, 461 F.3d 374, 383 (3d Cir. 2006). *Cf. Messerschmidt v. Millender*, 565 U.S. 535, 547 (2012) (“Where the alleged Fourth Amendment violation involves a search or seizure pursuant to a warrant, the fact that a neutral magistrate has issued a warrant is the clearest indication that the officers acted in an objectively reasonable manner or, as we have sometimes put it, in ‘objective good faith.’” (citing *United States v. Leon*, 468 U.S. 897, 922-923 (1984))). To survive a motion

to dismiss a claim that a warrant was issued on the basis of a false affidavit, as Plaintiffs assert here, Second Am. Compl. ¶ 127, a plaintiff must allege facts that would establish, under *Franks v. Delaware*, 438 U.S. 154 (1978), that the affidavit supporting issuance of the search warrant “contained a false statement which was made knowingly or with reckless disregard for the truth,” and that the false statement was “material to the finding of probable cause.” *Yusuf*, 461 F.3d at 383 (citation omitted); *see, e.g., Eaton v. Tosti*, No. CIV.09-5248 (WJM), 2010 WL 2483318, at \*6 (D.N.J. June 4, 2010) (stating this rule in a § 1983 case).

This same standard applies where a plaintiff claims a Fourth Amendment violation based on allegations that a search or seizure was conducted pursuant to a FISA order issued on the basis of a false statements. Courts, including the Third Circuit, have uniformly held that FISA’s procedures for issuance of “warrant-like” orders authorizing surveillance based on FISA’s foreign-intelligence-related probable cause showing are reasonable under the Fourth Amendment. *United States v. Duka*, 671 F.3d 329, 341, 343–45 (3d Cir. 2011); *see United States v. Abu-Jihaad*, 630 F.3d 102, 128–29 (2d Cir. 2010); *United States v. Ning Wen*, 477 F.3d 896, 898–99 (7th Cir. 2007); *United States v. Damrah*, 412 F.3d 618, 625 (6th Cir. 2005); *United States v. Johnson*, 952 F.2d 565, 573 (1st Cir. 1991); *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987); *United States v. Cavanagh*, 807 F.2d 787, 790–91 (9th Cir. 1987). Thus, as with criminal warrants, “the representations and certifications submitted in support of an application for [a FISA order] should be presumed valid” unless the aggrieved party makes the two-part *Franks* showing. *Abu-Jihaad*, 630 F.3d at 130; *see also United States v. Aziz*, 228 F. Supp. 3d 363, 371 (M.D. Pa. 2017) (“Courts within the Third Circuit and elsewhere have assumed, without deciding, that

*Franks*’ [sic] underlying principles apply in the FISA context.”); *United States v. Huang*, 15 F. Supp. 3d 1131, 1142 (D.N.M. 2014) (standard for *Franks* hearing not met where the defendant did not offer “anything more than conclusory speculations about allegations of falsehoods in the FISA affidavit”); *United States v. Mubayyid*, 521 F. Supp. 2d 125, 130 (D. Mass. 2007) (“The Court assumes that *Franks*, or at least its underlying principle, applies in [the FISA] context.”).

Here, Plaintiffs’ claims that they were subjected to searches and seizures conducted pursuant to search warrants and FISA orders issued without probable cause, on the basis of false affidavits or certifications, consist entirely of threadbare recitals of the elements of the cause of action, supported by mere conclusory statements. *See* Second Am. Compl. ¶¶ 59, 67, 125–130. Plaintiffs do not allege facts sufficient to support the reasonable inference that any statements in the affidavits or applications were knowingly false or made with reckless disregard for the truth, or that the statements were material to the finding of probable cause. *See Yusuf*, 461 F.3d at 383. Accordingly, Plaintiffs fail to state a claim that any search or seizure conducted pursuant to a search warrant or FISA order violated their Fourth Amendment rights. *See Iqbal*, 556 U.S. at 678; *see, e.g., Bey v. Genano*, No. PWG-16-2800, 2017 WL 1315530, at \*3 (D. Md. Apr. 10, 2017) (plaintiff failed to state a plausible Fourth Amendment claim where complaint did not “even specify which statements in the warrant affidavit were false”); *Moore v. City of New York*, No. 08-CV-2449 RRM LB, 2011 WL 795103, at \*6 (E.D.N.Y. Feb. 28, 2011) (plaintiff’s “conclusory and speculative” allegation that officer “signed a ‘bogus’ affidavit in support of [a] search warrant” was not entitled to a presumption of truth for purpose of deciding whether to grant a motion to dismiss); *Wag-Aero, Inc. v. United States*, 837 F. Supp. 1479, 1492 (E.D. Wis.

1993) (holding that, under *Franks* standard, a plaintiff claiming a Fourth Amendment violation must specifically plead the allegations in the warrant affidavit that are claimed to be false), *aff'd*, 35 F.3d 569 (7th Cir. 1994); *see also Sheare v. Borough of Olyphant*, No. 3:11-CV-1639, 2012 WL 140233, at \*4 (M.D. Pa. Jan. 18, 2012) (finding that plaintiffs' allegations were "only a threadbare recital of the elements of a § 1983 false arrest claim" where the complaint did not identify the alleged falsehoods in the warrant affidavit or state how the affiant disregarded the truth).

**C. Xi Does Not Plausibly Allege that the Government Violated His Fourth Amendment Rights Through Warrantless Surveillance Under FISA Section 702 or EO 12,333.**

Plaintiffs' remaining claim is that the Official Capacity Defendants, pursuant to the authority of FISA Section 702 "and/or" EO 12,333, Second Am. Compl. ¶ 60, "caus[ed] the interception of [ ] Xi's communications . . . without obtaining a warrant and without notice" in violation of Xi's Fourth Amendment rights. Second Am. Compl. ¶ 131. This claim fails to pass muster under Rule 12(b)(6) because Xi does not plausibly allege that his communications were even intercepted through warrantless surveillance under either of those authorities. Nor does Xi allege facts that would allow the reasonable inference that such surveillance, even if it occurred, violated his Fourth Amendment rights. Finally, Xi does not state a plausible Fourth Amendment claim based on alleged querying of databases containing information collected pursuant to Section 702 and EO 12,333.

**1. Xi Does Not Plausibly Allege that His Fourth Amendment Rights Were Violated by Warrantless Surveillance Under FISA Section 702.**

Xi does not plausibly allege that his communications were intercepted through warrantless surveillance under Section 702, let alone that such surveillance violated the Fourth Amendment.

**a. Xi Does Not Plausibly Allege that His Communications Were Intercepted Through Surveillance Under Section 702.**

As set forth above, the Government provided notice to Xi that it anticipated using information in his criminal case that was obtained through or derived from physical searches or electronic surveillance pursuant to 50 U.S.C. §§ 1801-1812 and 1821-1829. *See* FISA Notice at 1. These FISA provisions do not include Section 702, 50 U.S.C. § 1881a. Nonetheless, Xi alleges “[o]n information and belief” that Government agents “caused the interception of [ ] Xi’s communications . . . without obtaining a warrant from any court” under FISA Section 702 “and/or” EO 12,333 “both before and after obtaining the FISA orders.” Second Am. Compl. ¶ 60. Xi does not further specify when this alleged warrantless surveillance occurred; he does not identify whether the alleged warrantless surveillance was conducted pursuant to Section 702, EO 12,333, or both; and he does not identify which of his communications were allegedly intercepted through this alleged surveillance, vaguely suggesting that the communications included “emails, text messages, and/or phone calls.” *Id.* ¶ 60.

Instead, Xi asks the Court to infer that his communications were intercepted through warrantless surveillance based on broad and vague allegations regarding warrantless surveillance of Chinese universities and research institutions generally. *Id.* ¶¶ 61-63. With respect to Section 702, Xi merely alleges that “the Government has obtained certifications under Section 702 that specifically authorize warrantless surveillance related to the Chinese government and its components.” *Id.* ¶ 61. Even if this speculative allegation is credited, it does not plausibly allege that Xi’s communications were intercepted through such surveillance, as it does not identify which Chinese-government-related selectors were targeted, specify the time period during which those selectors were targeted, or allege that

Xi was communicating during that time period with individuals associated with those selectors.

Nor does Xi plausibly allege that his communications were intercepted through Section 702 surveillance by pointing to the Government’s reliance on emails between Xi and scientists working in China. Xi alleges (1) that Special Agent Haugen “referenced intercepted emails between [ ] Xi and scientists at Tsinghua University” and (2) that “all four of the emails relied upon by the Government in its dismissed indictment were emails between [ ] Xi and scientists working at Chinese research institutions,” and those institutions were allegedly connected by “computers, servers, and network backbones” subject to warrantless surveillance during an unspecified time period. Second Am. Compl. ¶¶ 61-62. However, the allegations merely support an inference that copies of Xi’s emails with the Chinese scientists were acquired pursuant to *some* legal authority. In sum, Xi’s allegations might be “consistent with” the interception of Xi’s communications through Section 702 surveillance, but they do not “allow[ ] the court to draw the reasonable inference” that Xi’s communications were in fact intercepted through such surveillance, let alone that the Government is liable for a Fourth Amendment violation. *Iqbal*, 556 U.S. at 678.

The Third Circuit’s decision in *Schuchardt v. President of the United States*, 839 F.3d 336 (3d Cir. 2016), is of no help to Xi in this regard. In *Schuchardt*, the Court of Appeals concluded that the plaintiff survived a facial standing challenge with respect to his claim seeking injunctive relief based on “the Government’s alleged bulk collection of online communications under PRISM,” *id.* at 341 n.3, because his allegations allowed the court to draw the reasonable inference that Schuchardt’s communications were

encompassed by such collection, satisfying Article III’s injury in fact requirement. *Id.* at 350. The *Schuchardt* court admitted that the PCLOB Report cited by the Government, and other authorities, “if correct” would “tend to undermine Schuchardt’s ability to show that his own electronic communications were seized by the PRISM program,” *id.* at 352, but concluded that it was inappropriate to consider those materials on a facial Rule 12(b)(1) motion, *id.* at 353. Here, in contrast, that same PCLOB Report is incorporated by reference in Plaintiffs’ complaint. *See* Second Am. Compl. ¶ 64 n.3. And in any case, Xi does not allege—let alone plausibly allege—that the Government is “intercepting, monitoring, and storing the content of *all or substantially all* of the e-mail sent by American citizens” through PRISM or any other program. *Schuchardt*, 839 F.3d at 341; *see also id.* at 354 n.13. Accordingly, the Third Circuit’s analysis in *Schuchardt* does not render plausible Xi’s allegation that his communications were intercepted through warrantless surveillance under Section 702.

**b. Xi Does Not Plausibly Allege that Any Purported Section 702 Surveillance Violated the Fourth Amendment.**

Even if Xi’s well-pleaded factual allegations allowed the Court to draw the reasonable inference that his communications were intercepted under FISA Section 702—which they do not—Xi would still fail to state a Fourth Amendment claim because he does not plausibly allege that any such surveillance constituted an unreasonable search or seizure under the Fourth Amendment.

The “touchstone” of the Fourth Amendment analysis “is always ‘the reasonableness in all the circumstances of the particular governmental invasion of a citizen’s personal security.’” *Pennsylvania v. Mimms*, 434 U.S. 106, 108-09 (1977) (per curiam) (quoting *Terry v. Ohio*, 392 U.S. 1, 19 (1968)). “[A]lthough ‘both the concept of probable cause and

the requirement of a warrant bear on the reasonableness of a search,” *New Jersey v. T.L.O.*, 469 U.S. 325, 340 (1985) (citation omitted), “neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance,” *Nat’l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 665 (1989). In fact, “the traditional probable-cause standard may be unhelpful” when the Government “seeks to *prevent*” dangers to public safety.” *Id.* at 668.

The Supreme Court has recognized exceptions to the warrant requirement in a variety of circumstances, including where “special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable,” *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987), and the needs are motivated “at [a] programmatic level” by other governmental objectives, *City of Indianapolis v. Edmond*, 531 U.S. 32, 48 (2000); *see id.* at 37-40.

In decisions both before and after FISA’s enactment, numerous courts, including the Third Circuit, have held that the Government’s special need for foreign-intelligence information justifies an exception to the warrant requirement. *See, e.g., Duka*, 671 F.3d at 341; *United States v. Butenko*, 494 F.2d 593, 605 (3d Cir. 1974) (en banc); *In re Directives Pursuant to Section 105B of FISA*, 551 F.3d 1004, 1010-12 (FISC Ct. Rev. 2008); *United States v. Truong Dinh Hung*, 629 F.2d 908, 912-16 (4th Cir. 1980). The rationale for these decisions derives from *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 322 (1972), a case involving electronic surveillance for domestic security purposes, *id.* at 299. Although the Supreme Court there held that “prior judicial approval” was required for “the type of domestic security surveillance” at issue in that case, *id.* at 324, the Court recognized that, due to the significant differences between the national-security investigations and



ordinary criminal investigations, different standards for intelligence surveillance “may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights” of citizens. *See id.* at 322-23; *Duka*, 671 F.3d at 339-41.

In concluding that no warrant is required in this context, the Third Circuit and other courts have emphasized the importance of the national interest in foreign-intelligence gathering above and beyond garden-variety law enforcement, as well as the need for flexibility in the timely collection of intelligence, given the particular nature and objectives of foreign-intelligence collection. *Duka*, 671 F.3d at 341; *Butenko*, 494 F.2d at 605; *In re Directives*, 551 F.3d at 1010-11; *Truong*, 629 F.2d at 912-14 (4th Cir. 1980); [Redacted Caption], 2011 WL 10945618, at \*24 (FISA Ct. Oct. 3, 2011); *United States v. Mohamud*, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at \*16-18 (D. Or. June 24, 2014) (“*Mohamud I*”), *aff’d*, 843 F.3d 420 (9th Cir. 2016) (“*Mohamud II*”), *cert. denied*, *Mohamud v. United States*, No. 17-5126, --- S.Ct. ---, 2018 WL 311442 (Mem) (Jan. 18, 2018).

Congress in fact enacted the FAA in 2008 in part because the burdens imposed on the Government’s limited intelligence resources and the delays occasioned by the requirement under then-current law to prepare individualized, probable-cause FISA applications for electronic surveillance targeting non-U.S. persons outside the United States were undermining the Government’s ability to collect foreign intelligence information. PCLOB Report at 18-20. A “significant purpose” of acquisitions under Section 702 must be, according to the statute’s terms, “to obtain foreign intelligence information,” 50 U.S.C. § 1881a(g)(2)(A)(v), such as information acquired to protect the

Nation against foreign attacks, international terrorism, international proliferation of weapons of mass destruction, and clandestine intelligence activities of foreign intelligence services. *See id.* § 1801(e); *see also In re Directives*, 551 F.3d at 1011 (Protect America Act of 2007 (“PAA”), the predecessor to the FAA, had the “stated purpose” of “garnering foreign intelligence” and “[t]here [was] no indication that the collections of information [were] primarily related to ordinary criminal-law enforcement purposes”). *Cf. In re Sealed Case*, 310 F.3d 717, 745-46 (FISC Ct. Rev. 2002) (“programmatic purpose” of obtaining foreign intelligence was “a special need”); *Cassidy v. Chertoff*, 471 F.3d 67, 82 (2d Cir. 2006) (interest in preventing terrorist attacks goes “well beyond” law enforcement).

The courts have also long recognized that “attempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy,” *Truong*, 629 F.2d at 913, and that conditioning acquisitions of foreign-intelligence information targeted at non-U.S. persons located overseas on obtaining a warrant would “hinder the government’s ability to collect time-sensitive” foreign intelligence, and thus “impede the vital national security interests that are at stake,” *In re Directives*, 551 F.3d at 1011. Courts considering the issue have found, in particular, that “application of the warrant requirement would [also] be impracticable” for acquisitions under Section 702. *Mohamud I*, 2014 WL 2866749, at \*18; *see also* [Redacted Caption], 2011 WL 10945618, at \*24.

Moreover, courts examining Section 702 surveillance specifically have had little trouble approving of the absence of a warrant requirement because such surveillance targets only non-U.S. persons located outside the United States. *See Mohamud II*, 843 F.3d at 439 (explaining that “the Fourth Amendment does not apply to searches and seizures by the United States against a non-resident alien in a foreign country” (quoting *United States*

*v. Zakharov*, 468 F.3d 1171, 1179 (9th Cir. 2006) (citing *United States v. Verdugo-Urquidez*, 494 U.S. 259, 274–75 (1990)); *United States v. Hasbajrami*, No. 11-cr-623 (JG), 2016 WL 1029500, at \*7 (E.D.N.Y. Mar. 8, 2016) (same); *see also United States v. Muhtorov*, 187 F. Supp. 3d 1240, 1254 (D. Colo. 2015) (“On its face, § 702 targets individuals *outside* the United States ‘to acquire foreign intelligence information.’ The reasonableness of that targeting, without a warrant, is not the essence of our inquiry.”).

Further, the surveillance activities authorized by Section 702 are reasonable. Even where a warrant and probable cause are not required, searches and seizures remain subject to the Fourth Amendment’s “traditional standards of reasonableness.” *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013). A court evaluating the reasonableness of particular foreign intelligence surveillance activities must consider the “totality of the circumstances,” *Samson v. California*, 547 U.S. 843, 848 (2006), weighing “the promotion of legitimate governmental interests against the degree to which [the activities] intrude[ ] upon” Plaintiffs’ protected Fourth Amendment interests, *King*, 133 S. Ct. at 1970. Applying this test, the FISA Court of Review found foreign-intelligence collection under the PAA reasonable, *In re Directives*, 551 F.3d 1012-15, and the Ninth Circuit recently found reasonable (and thus constitutional) electronic surveillance under Section 702’s PRISM program that entailed the incidental collection of a U.S. person’s communications, “even assuming [the U.S. person] had a Fourth Amendment right in the incidentally collected communications.” *Mohamud II*, 843 F.3d at 444; *see id.* at 438 & n.19.

The Government’s national-security interest in conducting acquisitions pursuant to Section 702 “is of the highest order of magnitude.” *In re Directives*, 551 F.3d at 1012; [Redacted Caption], 2011 WL 10945618, at \*25 (same). To be weighed against the

promotion of the compelling Government interest in protecting national security is the potential intrusion on U.S.-persons' Fourth Amendment interests through the incidental collection of their communications when non-U.S.-person-associated selectors are targeted under Section 702. Any such intrusion is limited because "[s]urveillance under [Section 702] is subject to statutory conditions, judicial authorization, congressional supervision, and compliance with the Fourth Amendment." *Amnesty Int'l*, 568 U.S. at 404; *see* PCLOB Report at 41-77, and this "matrix of [statutory] safeguards," *In re Directives*, 551 F.3d at 1013, contributes further to the program's reasonableness. *Cf. King*, 133 S. Ct. 1979-80 (statutory protections guarding against further invasion of privacy contribute to reasonableness).

In particular, the privacy interests of U.S. persons whose communications are incidentally intercepted in the course of Section 702 acquisition are protected through minimization procedures, which must be approved by the FISC. *See* 50 U.S.C. § 1881a(c)(1), (e). By definition, minimization procedures under FISA must be reasonably designed to minimize acquisition and retention, and to prohibit dissemination, of private information concerning U.S. persons, to the extent consistent with the Government's need to obtain, produce, and disseminate foreign intelligence information. *Id.* § 1801(h). Such minimization procedures have been held constitutionally sufficient to protect third-parties in the domestic law enforcement context. *See, e.g., United States v. Figueroa*, 757 F.2d 466, 471 (2d Cir. 1985) ("Innocent parties are protected from unreasonable surveillance by the requirement contained in [Title III] that surveillance 'shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception.'"). This conclusion applies fully—if not more forcefully—in the foreign

intelligence context. *See, e.g., In re Sealed Case*, 310 F.3d at 740-41 (holding that FISA’s requirement of minimization procedures supports statute’s reasonableness). In addition, the statute protects against invasion of U.S. persons’ privacy interests by requiring prior FISC approval of all targeting procedures used in any Section 702 acquisition, 50 U.S.C. § 1881a(i)(2)(B), and by building in oversight of the Government’s implementation of the targeting procedures, *id.* § 1881a(g)(l). Moreover, it is clear that Section 702 surveillance qualifies as a “reasonably effective means” of advancing the Government’s goals in protecting the Nation’s security. *Bd. of Educ. Indep. Sch. Dist. No. 92 of Pottawatomie Cty. v. Earls*, 536 U.S. 822, 837-38 (2002); *see* PCLOB Report at 104-110.

Indeed, examining these factors, every court to have considered the question has concluded that Section 702’s safeguards and procedures sufficiently protect U.S. persons’ privacy interests and satisfy the Fourth Amendment’s reasonableness standard. *See Mohamud II*, 843 F.3d at 441-44; *Hasbajrami*, 2016 WL 1029500, at \*10-13; *Muhtorov*, 187 F. Supp. 3d at 1254-58; *Mohamud I*, 2014 WL 2866749, at \*19-27.

Accordingly, the Government’s procedures for surveillance under Section 702 are compatible with the Fourth Amendment, and even if Xi’s speculative assertion that his communications were intercepted under Section 702 is credited, Xi does not plausibly allege that the Government failed to follow those procedures. Indeed, while Plaintiffs allege that the Government “regularly” fails to give statutorily required notice to criminal defendants when it “uses information obtained or derived from” surveillance under Section 702 in criminal proceedings, Second Am. Compl. ¶ 66, and that the Government “frequently rel[ies]” on Section 702 collection “to obtain without a warrant the communications of Americans,” *id.* ¶ 60, in violation of the statute’s prohibition on reverse

targeting, those allegations are not plausible in light of the PCLOB Report findings. *See, e.g.*, PCLOB Report at 163 (“The hurdles imposed by these existing requirements result in Section 702 information being used rarely in the prosecution of even national security–related crimes, and perhaps never in the prosecution of other crimes.”); *id.* at 79 (noting that, “[s]ince the Section 702 program’s inception, the compliance programs have . . . identified [only] two instances of reverse targeting,” the first of which resulted in acquisition of communications that were subsequently purged, and the second of which did not result in any communications being acquired); *id.* at 118 (noting that “the DOJ/ODNI oversight team has not discovered any instances in which an analyst intentionally violated the statute, targeting procedures, or minimization procedures”). And even if such allegations are taken as true, they would not “allow[ ] the [C]ourt to draw the reasonable inference” either that Xi’s own communications were in fact intercepted under Section 702 or that the Government departed from statutory or Fourth Amendment requirements in Xi’s case specifically. *Iqbal*, 556 U.S. at 678.

Xi has therefore failed to demonstrate that the Government violated his Fourth Amendment rights through warrantless surveillance under FISA Section 702.

## **2. Xi Does Not Plausibly Allege that the Government Violated His Fourth Amendment Rights by Conducting Surveillance Under EO 12,333.**

In addition to surmising that the Government acquired copies of his communications through surveillance under Section 702, Xi speculates that the Government may have intercepted his communications through surveillance conducted under EO 12,333. This tentative, alternative allegation that Xi’s communications were subject to surveillance under EO 12,333 is as speculative as the allegation that his communications were intercepted via Section 702 surveillance, and does not support the

reasonable inference that any such surveillance in fact occurred, let alone that it violated Xi's Fourth Amendment rights.

As with Section 702, Xi's suggestion that his communications may have been intercepted pursuant to EO 12,333 rests on broad, general allegations regarding warrantless surveillance of Chinese governmental entities. *See* Second Am. Compl. ¶¶ 61-64. For example, Xi alleges that (1) the Government had access to emails between Xi and scientists working at Tsinghua University, Peking University, and Shanghai Jiatong University, (2) during an unspecified time period prior to Xi's arrest, Tsinghua University was a location "where the NSA siphoned data off of computers, servers and network backbones," and (3) these "computers, servers, and network backbones carr[ied] the communications of tens of millions of people and connecting thousands of other Chinese research institutions, including Peking University and Shanghai Jiaotong University." *Id.* ¶¶ 61-62. Even if the Court credited the allegation that Tsinghua University was subject to such warrantless surveillance, *id.* ¶ 61,<sup>8</sup> Xi does not plausibly allege that his communications were intercepted through that surveillance, as Xi does not specify when "prior to [ ] Xi's arrest" this surveillance occurred, *id.*, the manner in which data was "siphoned . . . off," *id.*, or which communications were intercepted.

---

<sup>8</sup> Plaintiffs do not specifically identify whether this alleged surveillance at Tsinghua University was conducted pursuant to EO 12,333. But to the extent Plaintiffs allege that the "NSA" conducted warrantless surveillance *at* Tsinghua University under *Section 702* by "siphon[ing] data off of computers, servers, and network backbones carrying the communications of tens of millions of people and connecting thousands of other Chinese research institutions," Second Am. Compl. ¶ 61, that allegation is itself implausible since, as explained above, collection under Section 702 occurs in the United States, and involves the acquisition of communications by U.S.-based electronic communications service providers. *See* PCLOB Report at 33-37.

As noted above, the Government’s alleged possession of copies of communications between Xi and scientists working at the three listed universities allows the reasonable inference only that the communications were acquired pursuant to *some* authority—which could be, for example, a traditional FISA order. *See supra* at 26. Xi’s allegations, again, are at best merely consistent with a claim that Xi’s communications could have been intercepted through surveillance under EO 12,333, which is not sufficient to allow the Court to draw the reasonable inference that such surveillance in fact occurred. *See Iqbal*, 556 U.S. at 678.

Xi’s allegation that the Government has engaged in warrantless surveillance of Chinese universities and research institutions that has included “collection of communications in bulk,” Second Am. Compl. ¶ 61, likewise does not allow the reasonable inference that Xi’s communications were intercepted pursuant to surveillance under EO 12,333,<sup>9</sup> as Plaintiffs do not specify when this alleged bulk collection occurred, which data systems or networks it targeted, or in what sense “virtually *all* messages and data” on those systems or networks were “captured,” *id.*, let alone plausibly allege that Xi’s communications resided on the relevant system or network.

Moreover, even if the Court were to credit Xi’s implausible allegation that his communications were intercepted through surveillance of Chinese governmental entities under EO 12,333, Xi again fails to plausibly allege that such surveillance violated the Fourth Amendment. Collection under EO 12,333 is explicitly limited to foreign

---

<sup>9</sup> Although Xi again does not specifically allege the authority under which this alleged “bulk” collection purportedly occurred, he alleges in a footnote that “[t]he government has acknowledged that it engages in the bulk interception and collection of communications under [EO] 12,333,” Second Am. Compl. ¶ 61 n.1, and, as set forth in the PCLOB Report, Section 702 programs do not involve bulk collection. *See* PCLOB Report at 111-12.



intelligence and counterintelligence. *See, e.g.*, EO 12,333, § 1.7(c)(1) (NSA), *id.* § 1.7(g)(1) (intelligence elements of FBI). As discussed above, *see supra* at 28-30, the Third Circuit—and other courts—have uniformly held foreign intelligence collection falls within an exception to the warrant requirement. Xi does not allege—let alone plausibly allege—that his communications were captured through warrantless surveillance that was undertaken for a non-foreign-intelligence purpose. Nor does he allege that his communications were intercepted by warrantless surveillance under EO 12,333 conducted in the United States or that such surveillance targeted him or any other U.S. person. Xi’s allegations thus offer no reasonable basis to conclude that any alleged warrantless surveillance undertaken pursuant to EO 12,333 was unconstitutional.

**3. Xi Does Not Plausibly Allege that the Government Violated His Fourth Amendment Rights by Querying Databases Containing Information Collected Pursuant to Section 702 or EO 12,333.**

For the reasons explained above, *see supra* at 25-27, 34-36, Xi does not plausibly allege any of his communications were intercepted through surveillance under Section 702 or EO 12,333. Accordingly, he also has not plausibly alleged that the Official Capacity Defendants accessed or used communications between Xi and Chinese scientists collected under these authorities. *See* Second Am. Compl. ¶¶ 64-65. In any case, even if Xi’s communications were intercepted through warrantless surveillance, and even if that surveillance was unlawful, the Government would not violate the Fourth Amendment by storing the communications in databases, or otherwise “examining, retaining, [or] using” those communications, *id.* ¶ 132, as any Fourth Amendment violation was “fully accomplished by the original search.” *Calandra*, 414 U.S. at 354; *see, e.g., Mohamud I*, 2014 WL 2866749, at \*26 (concluding that “subsequent querying of a § 702 collection,

even if U.S. person identifiers are used, is not a separate search”).<sup>10</sup> Thus, Xi also fails to state a plausible Fourth Amendment claim based on his allegation that the Government, without obtaining a warrant, queried law enforcement databases containing copies of communications intercepted through warrantless surveillance under Section 702 or EO 12,333.

### CONCLUSION

For the foregoing reasons, the Court should dismiss Plaintiffs’ claims against the Official Capacity Defendants pursuant to Rule 12(b)(1) and Rule 12(b)(6).

---

<sup>10</sup> Similarly, for reasons explained above, *see supra* at 15-16, the Government does not violate the Fourth Amendment by retaining or using information acquired via a search conducted pursuant to a criminal search warrant or FISA order, even if such order or warrant was issued without probable cause. *See Calandra*, 414 U.S. at 354 (Fourth Amendment wrong “is fully accomplished by the original search without probable cause”); *Jacobsen*, 466 U.S. at 113 (Fourth Amendment seizure requires “meaningful interference” with possessory interests in property). Thus, even apart from their failure to plausibly allege that the underlying searches or seizures violated the Fourth Amendment, Plaintiffs do not state a claim that the Government violated the Fourth Amendment through the “retention of . . . information [ ] obtained through unlawful searches and seizures.” Second Am. Compl. ¶ 135.

Dated: February 2, 2018

Respectfully submitted,

CHAD A. READLER  
Acting Assistant Attorney General  
Civil Division

ANTHONY J. COPPOLINO  
Deputy Director  
Civil Division, Federal Programs Branch

/s/ Elizabeth Tulis  
ELIZABETH TULIS  
(NY Bar, under LCvR 83.5(e))  
Trial Attorney  
United States Department of Justice  
Civil Division, Federal Programs Branch  
P.O. Box 883  
Washington, D.C. 20044  
(202) 514-9237 (phone)  
(202) 616-8470 (fax)  
E-mail: elizabeth.tulis@usdoj.gov

*Attorneys for Defendants Christopher A.  
Wray, Jefferson B. Sessions, III, and Adm.  
Michael S. Rogers*

**CERTIFICATE OF SERVICE**

I, Elizabeth Tulis, a Trial Attorney in the U.S. Department of Justice, Civil Division, Federal Programs Branch, certify that on February 2, 2018, I caused the preceding motion and memorandum to be served by ECF on all parties receiving ECF notifications in this case.

Dated: February 2, 2018

/s/ Elizabeth Tulis  
ELIZABETH TULIS